La protección de datos personales es un derecho fundamental de todas las personas físicas.

El 25 de mayo de 2016 entró en vigor el Reglamento General de Protección de Datos (RGPD) de la Unión Europea (UE) que sustituirá a la actual normativa vigente y que comenzará a aplicarse el 25 de mayo de 2018.

Este periodo de dos años tiene como objetivo permitir que las organizaciones de la UE que tratan datos de carácter personal vayan adaptándose al mismo.

El RGPD es una norma directamente aplicable que no requiere de normas internas de trasposición a cada Estado.

Desde el cumplimento de la LOPD, para adecuarse al RGPD se deben desarrollar las siguientes actividades:

1. Necesidad de identificar con precisión las finalidades y la base jurídica de los tratamientos de carácter personal que se llevan a cabo. Esta obligación no deriva sólo de la necesidad de cumplir con el principio de legalidad establecido en el RGPD, sino que viene impuesta por el hecho de que las finalidades o la base jurídica de los tratamientos son informaciones que deben proporcionarse a los interesados (arts. 13 y 14 RGPD).
2. La identificación de finalidades y base jurídica tiene exigencias adicionales en los casos en que se traten datos de los considerados como objeto de especial protección, que incluyen, entre otros, los datos sobre salud, ideología, religión o pertenencia étnica. El tratamiento de estos datos está, con carácter general, prohibido, y sólo podrá llevarse a cabo si es aplicable alguna de las excepciones previstas en el art. 9.2 del RGPD. Entre ellas pueden destacarse, a los efectos de este documento, el que el tratamiento sea necesario para satisfacer un interés público esencial, el que sea necesario para fines de prevención, asistencia sanitaria o salud pública, o que sea necesario para la gestión de los servicios de asistencia social, en todos los casos en los términos que establezca la legislación española o de la UE.
3. El interés público que justifican el tratamiento debe estar acreditado en una norma de rango legal.
4. En los casos en que la base jurídica de los tratamientos sea el consentimiento, éste deberá tener las características previstas por el RGPD, que exige que sea informado, libre, específico y otorgado por los interesados mediante una manifestación que muestre su voluntad de consentir o mediante una clara acción afirmativa. Los consentimientos conocidos como tácitos, basados en la inacción de los interesados, dejarán de ser válidos a partir de la fecha de aplicación del RGPD, incluso para tratamientos iniciados con anterioridad.
5. El RGPD (arts. 13 y 14) obliga a ofrecer una información que es más amplia que la actualmente exigida por la LOPD. Obliga, además, a que esta información se proporcione de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.
6. Para el ejercicio de derechos se deben establecer:
    - Mecanismos visibles, accesibles y sencillos, incluidos los medios electrónicos. Cuando se trate del ejercicio por medios electrónicos,

éstos deben incorporar procedimientos para verificar la identidad de los interesados que los utilizan.

- Procedimientos que permitan responder en los plazos previstos por el RGPD. En los casos que sean los encargados del tratamiento los que colaboren en la atención a las solicitudes de los interesados deben incluirse en los contratos.

7. El RGPD establece una obligación de control en la elección de los encargados de tratamiento que deben aplicar todos los responsables, contratando únicamente encargados que estén en condiciones cumplir con el RGPD.
8. El RGPD establece que la relación entre responsables y encargados deberá formalizarse mediante un contrato o un acto jurídico que vincule al encargado. El RGPD exige expresamente que tanto los contratos como los actos jurídicos deberán tener un contenido mínimo que excede del actualmente previsto por la normativa española de protección de datos.
9. La aplicación del RGPD para todo tratamiento (tanto existente como futuro) debe ser objeto de un análisis de riesgos.
10. Se reemplaza la obligación de notificar los ficheros y tratamientos de carácter personal a las autoridades de protección de datos (p.e. AEPD) por un registro de actividades de tratamiento, tanto para responsables como para encargados de tratamiento. El registro podrá organizarse sobre la base de las informaciones ya proporcionadas en las notificaciones de los ficheros existentes. El registro deberá mantenerse actualizado y a disposición de las citadas autoridades.
11. El Reglamento de desarrollo de la LOPD contiene previsiones específicas sobre medidas de seguridad de acuerdo al grado de sensibilidad del tipo de datos que se tratan. Por el contrario, el RGPD exige que las medidas de seguridad se adecúen al análisis de riesgos, es decir, a las características de los tratamientos, sus riesgos, el contexto en que se desarrollan, el estado de la tecnología y al coste.
12. Necesidad de establecer mecanismos para identificar con rapidez la existencia de violaciones de seguridad de los datos y reaccionar ante ellas, en particular para evaluar el riesgo que puedan suponer para los derechos y libertades de los afectados y para notificar esas violaciones de seguridad a las autoridades de protección de datos y, si fuera necesario, a las personas afectadas. El RGPD establece, asimismo, la obligación de mantener un registro de todos los incidentes de seguridad, sean o no objeto de notificación.
13. El RGPD establece que, con anterioridad a su puesta en marcha, los tratamientos que sea probable que supongan un alto riesgo para los derechos y libertades de los afectados deberán ser objeto de una evaluación de impacto sobre la protección de datos con un contenido mínimo. El RGPD determina algunos de los casos en que se presumirá que existe ese alto riesgo y prevé que las autoridades de protección de datos publiquen listas de otros tratamientos de alto riesgo.
14. El RGPD prevé que se nombre un delegado de protección de datos (DPD) en el caso de las AAPP, cuando se realicen tratamientos de datos personales a gran escala, datos especiales (salud, ideología, religión o pertenencia étnica) y/o datos relativos a condenas e infracciones penales. La designación del DPD

debe comunicarse a las autoridades de protección de datos. Asimismo, deben establecerse mecanismos para que las personas interesadas puedan contactar con el DPD.

15. El RGPD mantiene el modelo de transferencias internacionales ya existente, pero amplía el catálogo de instrumentos para ofrecer garantías suficientes que no requerirán de autorización previa de las autoridades de protección de datos.